PPG

UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/760,434	01/12/2001	Boby Joseph	00-551	2877

20306 7590 07/29/2004

MCDONNELL BOEHNEN HULBERT & BERGHOFF LLP
300 S. WACKER DRIVE
32ND FLOOR
CHICAGO, IL 60606

EXAMINER	
VAUGHAN, MICHAEL R	
ART UNIT	**PAPER NUMBER**
2131	

DATE MAILED: 07/29/2004

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)	
	09/760,434	JOSEPH ET AL.	
	Examiner	Art Unit	
	Michael R Vaughan	2131	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE *3* MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *12 January 2001*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-27* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-27* is/are rejected.

7)☒ Claim(s) *16-22 and 24-27* is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on *12 January 2001* is/are: a)☒ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☒ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) Paper No(s)/Mail Date *6-25-01*.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other: _____.

DETAILED ACTION

Claims 1-27 have been examined and are pending.

Information Disclosure Statement

An initialed and dated copy of Applicant's IDS form 1449, Paper Filed 6-25-01, is attached to the instant Office action.

Claim Objections

Claims 16-22 and 24-27 are objected to because of the following informalities: each adds a step in the method by reciting, "comprising the step of". None of the steps have been previously define so "the" should be –a--. Appropriate correction is required.

Claim Rejections - 35 USC ' 112, second paragraph

Claims 2-6 are rejected under 35 U.S.C. 112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which applicant regards as the invention. Claim 6 recites the limitation "the security information" but there is insufficient antecedent basis. Clarification and/or correction are required.

Claims 11-14 are rejected under 35 U.S.C. 112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which applicant regards as the invention. Claim 11 recites the limitation "the security information" but there is insufficient antecedent basis. Clarification and/or correction are required.

Claim Rejections - 35 USC ' 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject

matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

Claims 1- are rejected under 35 U.S.C. 103(a) as being unpatentable over Adelman et al, hereinafter Adelman (USP 6,006,259) in view of Thomas et al, hereinafter Thomas (USP 5,151,899).

As per claim 1, Adelman teaches: a first, a second, and a third network device (figures 2 and 4), a first secure communication between the first and second network devices (column 5, line 19), the first secure communication having a security association (column 4, lines 56-64) and the second secure communication having the same security association as the first secure (column 4, lines 56-64). The second secure communication is between the first network device and another of the devices present in figure 4.

Adelman teaches the each apparatus is able to filter incoming messages by unique index numbers (sequence numbers) in order to correctly identify all packets belonging to that particular apparatus (column 3, lines 1-30). Adelman uses generated index numbers but is silent in disclosing a predefined sequence number limit less than a maximum sequence number. Thomas teaches a predefined sequence number limit less than a maximum sequence number (column 7, lines 40-46). Thomas teaches in order to correctly track sequence numbers, it is computational more efficient to detect sequence numbers with bounds. In view of this it would have been obvious to one of

ordinary skill in the art at the time of the invention to employ the teachings of Thomas et al. within the system of Adelman because it would reduce the computations needed to constantly hash out index numbers. Adelman invention insists that apparatuses are able to quickly determine which packets need to be processed. By incorporating the bounded sequence numbers of Thomas, the invention must still be able to correctly assign certain packets to the proper receiving apparatus. The obvious solution when dealing with bounded sequence numbers is to assign a bounded range to each apparatus. Thus the second secure communication would have sequence numbers outside (including greater) than the limit of the first secure communication.

As per claim 2, Adelman teaches a fourth network device having security information corresponding to the security association, the fourth network device capable of passing the security information from the first network device to the third network device (column 4, lines 15-18).

As per claim 3, Adelman teaches the security information comprises at least a security parameter index (column 4, lines 55-62).

As per claim 4, Adelman teaches the fourth network device is a redundancy handler (column 4, line 16).

As per claim 5, Adelman teaches the fourth network device is a router (column 4, line 16).

As per claim 6, Adelman teaches the fourth network device is a media gateway controller, and the first and third network devices are media gateways (column 4, lines 15-30 and column 5, line 18).

As per claim 7, Adelman teaches the first and second network device are blades (cluster members, see column 2, lines 63-67).

As per claim 8, Adelman teaches the first network device is an active network device and the third network device is a standby network device (column 1, lines 62-63 and column 12, lines 15-20).

As per claim 9, Adelman teaches wherein the second secure communication replaces the first secure communication when the first secure communication fails (column 12, lines 15-20).

As per claim 15, Adelman teaches: a first secure communication between the first and second network devices (column 5, line 19), negotiating a security association for the first communication, the first secure communication having a security association (column 4, lines 56-64) and the second secure communication having the same security

association as the first secure (column 4, lines 56-64). Adelman teaches replacing the first communication with a second communication between the first and third network devices (column 12, lines 15-20). The second secure communication is between the first network device and another of the devices present in figure 4.

Adelman teaches the each apparatus is able to filter incoming messages by unique index numbers (sequence numbers) in order to correctly identify all packets belonging to that particular apparatus (column 3, lines 1-30). Adelman uses generated index numbers but is silent in disclosing a predefined sequence number limit less than a maximum sequence number. Thomas teaches a predefined sequence number limit less than a maximum sequence number (column 7, lines 40-46). Thomas teaches in order to correctly track sequence numbers, it is computational more efficient to detect sequence numbers with bounds. In view of this it would have been obvious to one of ordinary skill in the art at the time of the invention to employ the teachings of Johnson within the system of Adelman because it would reduce the computations needed to constantly hash out index numbers. Adelman invention insists that apparatuses are able to quickly determine which packets need to be processed. By incorporating the bounded sequence numbers of Thomas, the invention must still be able to correctly assign certain packets to the proper receiving apparatus. The obvious solution when dealing with bounded sequence numbers is to assign a bounded range to each apparatus. Thus the second secure communication would have sequence numbers outside (including greater) than the limit of the first secure communication.

As per claim 16, Adelman teaches passing the security information corresponding to the security association from the first to the third network device (column 2, lines 33-36). Adelman's system is able to pick up a communication if the first network device fails without requiring the client to reconnect. This implies that the state of the connection is preserved and the client does not have to then re-authenticate or reestablish a session key.

As per claim 17, Adelman teaches the security information comprises at least a security parameter index (column 4, lines 55-62).

As per claim 19, Adelman teaches wherein the second secure communication replaces the first secure communication when the first secure communication fails (column 12, lines 15-20).

As per claim 22, Adelman teaches the first second and third network device are blades (cluster members, see column 2, lines 63-67).

As per claim 23, Adelman teaches: a first secure communication between the first and second network devices (column 5, line 19), negotiating a security association for the first communication, the first secure communication having a security association (column 4, lines 56-64) and the second secure communication having the same security association as the first secure (column 4, lines 56-64). Adelman teaches replacing the first communication with a second communication between the first and third network

devices (column 12, lines 15-20). The second secure communication is between the first network device and another of the devices present in figure 4.

Adelman teaches the each apparatus is able to filter incoming messages by unique index numbers (sequence numbers) in order to correctly identify all packets belonging to that particular apparatus (column 3, lines 1-30). Adelman uses generated index numbers but is silent in disclosing a predefined sequence number limit less than a maximum sequence number. Thomas teaches a predefined sequence number limit less than a maximum sequence number (column 7, lines 40-46). Thomas teaches in order to correctly track sequence numbers, it is computational more efficient to detect sequence numbers with bounds. In view of this it would have been obvious to one of ordinary skill in the art at the time of the invention to employ the teachings of Johnson within the system of Adelman because it would reduce the computations needed to constantly hash out index numbers. Adelman invention insists that apparatuses are able to quickly determine which packets need to be processed. By incorporating the bounded sequence numbers of Thomas, the invention must still be able to correctly assign certain packets to the proper receiving apparatus. The obvious solution when dealing with bounded sequence numbers is to assign a bounded range to each apparatus. Thus the second secure communication would have sequence numbers outside (including greater) than the limit of the first secure communication.

Adelman teaches passing the security information corresponding to the security association from the first to the third network device (column 2, lines 33-36). Adelman's system is able to pick up a communication if the first network device fails without

requiring the client to reconnect. This implies that the state of the connection is preserved and the client does not have to then re-authenticate or reestablish a session key.

As per claim 24, Adelman teaches the security information comprises at least a security parameter index (column 4, lines 55-62).

As per claim 25, Adelman teaches wherein the second secure communication replaces the first secure communication when the first secure communication fails (column 12, lines 15-20).

Claim 10, 13, 18, 20, 26, and 27 are rejected under 35 U.S.C. 103(a) as being unpatentable over Adelman and Thomas as applied to claim 1 above, and further in view of Medvinsky (WO 00/62507).

As per claims 10, 20, and 26, Adelman is silent in disclosing that replay prevention is enabled. Adelman does teach that the user has private cryptographically information to create secure communication with the network apparatuses. Medvinsky teaches a secure communication in which timestamps are used to check for replays of all messages (page 5, lines 25-26). In view of this it would have been obvious to one of ordinary skill in the art at the time of the invention to employ the teachings of Medvinsky within the system of Adelman because it would prevent secure communication messages from being replayed to exploit the system.

As per claims 18 and 27, Adelman is silent in disclosing that the security information is stored on a fourth network device. Medvinsky teaches storing security information on a network node whereby it can be retrieved and used to generate security associations (page 3, lines 10-13). In view of this it would have been obvious to one of ordinary skill in the art at the time of the invention to employ the teachings of Medvinsky within the system of Adelman because it would assist in generating a secure communication through the use of security information.

As per claim 13, Adelman is silent in disclosing the first and secure communication are voice calls. Medvinsky teaches implementing secure voice calls over a digital network (see abstract). In view of this it would have been obvious to one of ordinary skill in the art at the time of the invention to employ the teachings of Medvinsky within the system of Adelman because it would extend the data messages to encapsulating voice over IP as well.

Claim 11-14 are rejected under 35 U.S.C. 103(a) as being unpatentable over Adelman in view of Thomas in view of Medvinsky.

As per claim 11, Adelman teaches: a first, a second, and a third network device (figures 2 and 4), a first secure communication between the first and second network

devices (column 5, line 19), the first secure communication having a security association (column 4, lines 56-64) and the second secure communication having the same security association as the first secure (column 4, lines 56-64). The second secure communication is between the first network device and another of the devices present in figure 4.

Adelman teaches the each apparatus is able to filter incoming messages by unique index numbers (sequence numbers) in order to correctly identify all packets belonging to that particular apparatus (column 3, lines 1-30). Adelman uses generated index numbers but is silent in disclosing a predefined sequence number limit less than a maximum sequence number. Thomas teaches a predefined sequence number limit less than a maximum sequence number (column 7, lines 40-46). Thomas teaches in order to correctly track sequence numbers, it is computational more efficient to detect sequence numbers with bounds. In view of this it would have been obvious to one of ordinary skill in the art at the time of the invention to employ the teachings of Johnson within the system of Adelman because it would reduce the computations needed to constantly hash out index numbers. Adelman invention insists that apparatuses are able to quickly determine which packets need to be processed. By incorporating the bounded sequence numbers of Thomas, the invention must still be able to correctly assign certain packets to the proper receiving apparatus. The obvious solution when dealing with bounded sequence numbers is to assign a bounded range to each apparatus. Thus the second secure communication would have sequence numbers outside (including greater) than the limit of the first secure communication.

Adelman teaches a fourth network device having security information corresponding to the security association, the fourth network device capable of passing the security information from the first network device to the third network device (column 4, lines 15-18).

Adelman is silent in disclosing that replay prevention is enabled. Adelman does teach that the user has private cryptographically information to create secure communication with the network apparatuses. Medvinsky teaches a secure communication in which timestamps are used to check for replays of all messages (page 5, lines 25-26). In view of this it would have been obvious to one of ordinary skill in the art at the time of the invention to employ the teachings of Medvinsky within the system of Adelman because it would prevent secure communication messages from being replayed to exploit the system.

As per claim 12, Adelman teaches wherein the second secure communication replaces the first secure communication when the first secure communication fails (column 12, lines 15-20).

As per claim 13, Adelman is silent in disclosing the first and secure communication are voice calls. Medvinsky teaches implementing secure voice calls over a digital network (see abstract). In view of this it would have been obvious to one of ordinary skill in the art at the time of the invention to employ the teachings of

Medvinsky within the system of Adelman because it would extend the data messages to encapsulating voice over IP as well.

As per claim 14, Adelman teaches the security information comprises at least a security parameter index (column 4, lines 55-62).

Conclusion

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Michael R Vaughan whose telephone number is 703-305-0354. The examiner can normally be reached on M-F 7:30-4:00.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Ayaz Sheikh can be reached on 703-305-9648. The fax phone number for the organization where this application or proceeding is assigned is 703-872-9306.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

MV
Michael R Vaughan

Examiner

Art Unit 2131

AYAZ SHEIKH
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100